FILED
2015 Jul-20 PM 10:31
U.S. DISTRICT COURT
N.D. OF ALABAMA

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION

IN RE: COMMUNITY HEALTH SYSTEMS, INC., CUSTOMER SECURITY DATA BREACH LITIGATION (MDL 2595)	)	MASTER FILE NO. 15-CV-222-KOB
	)	THIS DOCUMENT RELATES TO ALL CASES

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs (identified below), by and through their undersigned counsel, individually and on behalf of all others similarly situated, file this Consolidated Amended Class Action Complaint against Community Health Systems, Inc. ("CHS") and Community Health Systems Professional Services Corporation ("CHSPSC") (collectively "CHS" or "Defendants"). This Consolidated Amended Class Action Complaint is filed to comply with the prior Orders of this Court (Doc. 14) (Doc. 22). In support thereof, based upon personal knowledge with respect to Plaintiffs and otherwise on information and belief derived from, among other things, investigation by counsel and review of public documents, Plaintiffs state and allege as follows:

NATURE OF THE ACTION

1. Through a network of affiliated physicians, hospitals and clinics, Defendants provide healthcare services to millions of individuals throughout the United States. Defendants maintain a centralized computer-based repository of confidential patient data for all of the patients who treat with and/or are referred to their vast healthcare network.

2. Inherent in a healthcare provider's relationship with a patient is the promise by the healthcare provider that all information divulged by the patient, as well as all information created by virtue of the patient's diagnosis and treatment, will, at all times, remain confidential.

This fundamental principal is embodied in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 29 U.S.C. §§ 1181 *et seq.*, and is a core component of the healthcare provider/patient relationship. Indeed, it is difficult to imagine any patient who would agree to accept treatment from a healthcare provider which did not promise to keep such information confidential.

3. The duty undertaken by healthcare providers to comply with HIPAA's requirements, and the concomitant promise to act reasonably to safeguard confidential patient data, is both an essential term of the contract for the provision of healthcare services and an industry standard of conduct.

4. This case is about Defendants' breach of that contract and violation of that industry standard of conduct.

5. Plaintiffs, current and former patients of Defendants' healthcare network, bring this class action on behalf of themselves and all other individuals whose confidential patient data, including personally identifiable information such as names, addresses, birthdates, telephone numbers, Social Security numbers, employer names, and guarantor names, as well as protected health information, was removed from the computer network of Defendants beginning in or about April 2014 (the "Data Breach").

6. Hackers first infiltrated Defendants' computer network on or about April 2014, but Defendants did not confirm the Data Breach until July 2014, and failed, in violation of HIPAA notification regulations and several state data breach notification statutes, to even begin notifying Plaintiffs and the members of the proposed classes, defined below, of the breach until August 2014.

7. As a result of Defendants' failure to adequately monitor their highly touted computer network, their use of a test server not intended to be connected to the Internet, and their failure to patch their computer system after the Heartbleed Vulnerability, a software flaw, was discovered, Plaintiffs' highly sensitive confidential patient data was easily extracted by unknown third parties.

8. This class action is brought by Plaintiffs to recover damages and to obtain equitable relief. Plaintiffs assert common law claims for breach of contract, breach of implied contract, unjust enrichment, negligence, negligence *per se*, bailment, and wantonness on behalf of a National Class, or, alternatively, if a National Class is not certified, on behalf of Alternate State Specific Classes, which are defined herein. Plaintiffs also assert federal statutory claims for violation of the Fair Credit Reporting Act on behalf of a National Class. Additionally, Plaintiffs assert claims under various state consumer protection and data breach notification laws, on behalf of State Statutory Classes, which are defined herein.

9. Defendants had a contractual and legal duty to protect, and accepted payment in exchange for their promise to protect, the private, highly sensitive, confidential patient data belonging to Plaintiffs and the members of the proposed classes.

10. Plaintiffs and the members of the proposed classes paid money to receive services from Defendants' healthcare network. A portion of those monetary payments was made for the protection of confidential patient data in Defendants' allegedly secure computer network. Because Defendants failed to secure and protect Plaintiffs' and class members' confidential patient data, Defendants' retention of fees paid for that security and protection is unjust, and represents an overpayment for which Plaintiffs and the members of the proposed classes should be compensated. Such overpayment constitutes monetary damages and economic loss.

11. Plaintiffs and the members of the proposed classes have a possessory interest in their confidential patient data and an interest in it remaining private because that information, including such incredibly private and sensitive information as Social Security numbers, has substantial value not only to Plaintiffs and the members of the proposed classes but to criminals who traffic in such information.

12. Because of the overpayment for data security that was not provided, the intrinsic value of the stolen information itself, the time and effort spent taking appropriate mitigating measures to avoid and/or respond to identity theft in the wake of the Data Breach, and the certain threat of immediate harm caused by the Data Breach, Plaintiffs and the members of the proposed classes have suffered a cognizable financial injury and monetary damages. This injury is a direct result of Defendants' failure to safeguard the confidential patient data of the Plaintiffs and the members of the proposed classes.

13. All Plaintiffs and members of the proposed classes have suffered monetary damages and economic loss by overpaying for CHS-provided healthcare that was to include appropriate data security, but ultimately did not include such security. Additionally, Plaintiffs and members of the proposed classes were harmed by having their confidential patient data misappropriated and made available to identity thieves. Many have suffered identity theft, fraud, and abuse, due to having their confidential patient data sold on the Internet black market resulting in monetary damages and economic loss, including but not limited to: unauthorized charges on bank and credit cards; fraudulently opened cards or accounts; emails hacked; impersonation by hackers with government agencies, credit card companies, and retailers; medical information stolen; cell phones and checking accounts hacked; fraudulent online payments; compromised credit scores; and fraudulent tax returns filed. All are at an increased

and certain risk of becoming victims of identity theft crimes, fraud, and abuse due to having confidential patient data sold on the Internet black market (which will result in the same aforementioned monetary damages and economic loss), and all have been forced to spend considerable time and money to investigate and mitigate the imminent risk of harm from identity theft, fraud, and abuse as a result of Defendants' conduct, including, but not limited to: detecting and preventing identity theft and unauthorized use of financial and/or medical information; monitoring accounts for fraudulent charges; canceling and obtaining reissued credit cards; dealing with the IRS and other government agencies; purchasing credit monitoring and identity theft protection services and insurance.

THE PARTIES

14. Plaintiff Kathy Ellzey ("Plaintiff Ellzey"), a resident of Hokes Bluff, Alabama, was treated at Gadsden Regional Hospital, a CHS facility, in April and August 2014. As part of the patient-admission process, Plaintiff Ellzey was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Ellzey's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Since the data breach at CHS, Plaintiff Ellzey has experienced unauthorized charges placed on her credit card, and has spent approximately 30 hours addressing the theft of her identity and has expended her own funds to cover postage expenses related to the data breach. Plaintiff Ellzey also believes that her email has been hacked. Plaintiff Ellzey has spent at least $5.00 on postage fees in connection with ramifications of the data breach. Plaintiff Ellzey faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

15. Plaintiff Patricia Ann McNutt ("Plaintiff McNutt"), a resident of Fort Payne, Alabama, was treated at Gadsden Regional Medical Center, affiliated with CHS, during the period April to June, 2013. As part of the patient-admission process, Plaintiff McNutt was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff McNutt's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Plaintiff McNutt faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

16. Plaintiff Lynda Matus ("Plaintiff Matus"), a resident of Bon Secour, Alabama, was treated at South Baldwin Regional Medical Center, a CHS facility, in June, 2012. As part of the patient-admission process, Plaintiff Matus was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Matus' confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Since the data breach at CHS, Plaintiff Matus has experienced the unauthorized opening of a charge card in her name, and has spent considerable time addressing issues with that account. To protect her identity going forward, Ms. Matus added identity theft protection through her bank, at a rate of $6.00 per month. Plaintiff Matus faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

17. Plaintiff Bobbie Jean Richard ("Plaintiff Richard"), a resident of Robertsdale, Alabama, was treated at the South Baldwin Regional Medical Center, and other CHS-affiliated

medical centers, from 2004 to the present. As part of the patient-admission process, Plaintiff Richard was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Richard's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Plaintiff Richard faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

18. Plaintiff Dallas Richard ("Plaintiff D-Richard"), a resident of Robertsdale, Alabama, was treated at the South Baldwin Regional Medical Center, and other CHS-affiliated medical centers, from 2004 to the present. As part of the patient-admission process, Plaintiff Richard was required to provide CHS with his confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff D-Richard's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and he suffered cognizable injury thereby. Since the data breach at CHS, Plaintiff D-Richard has experienced unauthorized charges placed on his credit card, and new financial accounts have been opened in his name. Plaintiff D-Richard has spent numerous hours addressing the theft of his identity and continues to do so. Plaintiff D-Richard faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of his confidential patient data, like all members of the proposed class.

19. Plaintiff Steve Percox ("Plaintiff Percox"), a resident of Tucson, Arizona, was treated at the Northwest Medical Center, affiliated with CHS, in 2010. As part of the patient-admission process, Plaintiff Percox was required to provide CHS with his confidential patient data, which CHS promised would be protected in accordance with industry standards and as

mandated by law. Plaintiff Percox' confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and he suffered cognizable injury thereby. Plaintiff Percox faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of his confidential patient data, like all members of the proposed class.

20. Plaintiff Sandra Arevalo ("Plaintiff Arevalo"), a resident of Rogers, Arkansas, was treated at a CHS-affiliated hospital, Northwest Medical Center, between 2003 and the present. As part of the patient-admission process, Plaintiff Arevalo was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Arevalo's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Plaintiff Arevalo faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

21. Plaintiff Todd Glass ("Plaintiff Glass"), a resident of Rogers, Arkansas, was treated at Northwest Medical Center in Springdale, Arkansas, a CHS-affiliated hospital, between 2005 and 2009. As part of the patient-admission process, Plaintiff Glass was required to provide CHS with his confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Glass' confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and he suffered cognizable injury thereby. Plaintiff Glass faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of his confidential patient data, like all members of the proposed class.

22. Plaintiff Martin Griffin ("Plaintiff Griffin"), a resident of Grant, Florida, was treated at a CHS-affiliated hospital, the Osler HMA Medical Group, between 2009 and 2014. As part of the patient-admission process, Plaintiff Griffin was required to provide CHS with his confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Griffin's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and he suffered cognizable injury thereby. Plaintiff Griffin faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of his confidential patient data, like all members of the proposed class.

23. Plaintiff Ashley Veciana ("Plaintiff Veciana"), a resident of Zephyrhills, Florida, sought treatment for her minor son at the CHS-affiliated facility now called Bayfront Health Dade City in October, 2013. As part of the patient-admission process, Plaintiff Veciana was required to provide CHS with her confidential data before they would treat her son, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Veciana's confidential data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Since the data breach at CHS, Plaintiff Veciana has experienced identity theft in the form of a hacking of her cell phone account with Metro PCS. Plaintiff Veciana faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential data, like all members of the proposed class.

24. Plaintiff Denise Bubel ("Plaintiff Bubel"), a resident of Grovetown, Georgia, was treated at Trinity Hospital of Augusta, Georgia, affiliated with CHS, in 2012. As part of the patient-admission process, Plaintiff Bubel was required to provide CHS with her confidential

patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Bubel's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. After receiving notice of the CHS data breach, Plaintiff Bubel purchased Life-Lock protection and after freezing her accounts to protect herself from identity theft, had to pay each time she unlocked her accounts to conduct financial transactions. Plaintiff Bubel faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

25. Plaintiff Richard Dale Floyd ("Plaintiff Floyd"), a resident of Mcleansboro, Illinois, was treated at Crossroads Community Hospital, a CHS-affiliated hospital, in 2013 and 2014. As part of the patient-admission process, Plaintiff Floyd was required to provide CHS with his confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Floyd's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and he suffered cognizable injury thereby. Plaintiff Floyd faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of his confidential patient data, like all members of the proposed class.

26. Plaintiff Vanessa Partridge ("Plaintiff Partridge"), a resident of San Pierre, Indiana, was treated at Porter Hospital, affiliated with CHS, in 2006, 2008 and 2014. As part of the patient-admission process, Plaintiff Partridge was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Partridge's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she

suffered cognizable injury thereby. Plaintiff Partridge faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

27. Plaintiff Daniel Watson ("Plaintiff Watson"), a resident of Fort Wayne, Indiana, was treated at Lutheran Hospital in Fort Wayne, between 2002 and the present. As part of the patient-admission process, Plaintiff Watson was required to provide CHS with his confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Watson's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and he suffered cognizable injury thereby. Since the data breach at CHS, Plaintiff Watson has experienced the unauthorized access of his checking account and the attempted theft of funds from his checking account. Plaintiff Watson added security to his checking account and put a freeze on all his financial accounts with the credit bureaus. Plaintiff Watson faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of his confidential patient data, like all members of the proposed class.

28. Plaintiff Lanetta Page ("Plaintiff Page"), a resident of Mayfield, Kentucky, was treated at a CHS-affiliated practice prior to the data breach. As part of the patient-admission process, Plaintiff Page was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Page's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Plaintiff Page faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

29. Plaintiff Joel Lovelace ("Plaintiff Lovelace"), a resident of Vidalia, Louisiana, treated at a facility affiliated with CHS prior to the CHS data breach. As part of the patient-admission process, Plaintiff Lovelace was required to provide CHS with his confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Lovelace's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and he suffered cognizable injury thereby. Since the data breach at CHS, Plaintiff Lovelace has experienced unauthorized charges placed on his credit card. Plaintiff Lovelace faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of his confidential patient data, like all members of the proposed class.

30. Plaintiff Melissa Cooper ("Plaintiff Cooper"), a resident of Jackson, Mississippi, was treated at Merit Health Center in Jackson, Mississippi and other CHS-affiliated facilities between 2005 and 2010. As part of the patient-admission process, Plaintiff Cooper was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Cooper's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Since the data breach at CHS, Plaintiff Cooper has experienced the hacking of her email account, the unauthorized opening of new financial accounts in her name, and the unauthorized use of online payment services. Plaintiff Cooper faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

31. Plaintiff Braquelle Lawson ("Plaintiff Lawson"), a resident of Utica, Mississippi, was treated at Merit Health Central in Jackson, Mississippi, a CHS-affiliated facility in March,

2013. As part of the patient-admission process, Plaintiff Lawson was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Lawson's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Plaintiff Lawson faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

32. Plaintiff Alan Wingard ("Plaintiff Wingard"), a resident of Parnell, Missouri, was treated at a CHS-affiliated hospital, North West Medical Center, in 2013. As part of the patient-admission process, Plaintiff Wingard was required to provide CHS with his confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Wingard's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and he suffered cognizable injury thereby. Plaintiff Wingard faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of his confidential patient data, like all members of the proposed class.

33. Plaintiff Johannes Nhete ("Plaintiff Nhete"), a resident of La Vista, Nebraska, was treated at a CHS-affiliated hospital, The Southside Regional Medical Center in Petersburg, Virginia, between 2003 and the present. As part of the patient-admission process, Plaintiff Nhete was required to provide CHS with his confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Nhete's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and he suffered cognizable injury thereby. Since the data breach at CHS,

Plaintiff Nhete has experienced the unauthorized use of his credit card, the hacking of his personal e-mail and cell phone, the unauthorized use of on-line payment services, and has found that someone tried to rent an apartment in his name in the state of Ohio. Plaintiff Nhete faces an ongoing, imminent, certainly impending threat of future additional harm in the theft of his confidential patient data, like all members of the proposed class.

34. Plaintiff Robert Burns ("Plaintiff Burns"), a resident of Woolwich Township, New Jersey, was treated at The Memorial Hospital of Salem County, NJ, affiliated with CHS, during the period 2005 to 2012. As part of the patient-admission process, Plaintiff Burns was required to provide CHS with his confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Burns' confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and he suffered cognizable injury thereby. Plaintiff Burns faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of his confidential patient data, like all members of the proposed class.

35. Plaintiff Jane Angel-Lopez ("Plaintiff Lopez"), a resident of Las Vegas, New Mexico, was treated at CHS-affiliated Alta Vista Regional Hospital prior to the CHS data breach. As part of the patient-admission process, Plaintiff Lopez was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Lopez' confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Plaintiff Lopez faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

36. Plaintiff Joan Crespin ("Plaintiff Crespin"), a resident of Las Vegas, New Mexico, was treated at CHS-affiliated Alta Vista Regional Hospital prior to the CHS data breach. As part of the patient-admission process, Plaintiff Crespin was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Crespin's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Since the data breach at CHS, Plaintiff Crespin had unauthorized charges placed on her credit cards from out-of-state sporting goods stores and a cheese store. In May 2015 someone used Plaintiff Crespin's credit card to charge hotel and flight reservations to Rio de Janeiro, Brazil. Plaintiff Crespin was forced to replace her credit cards on both occasions, expending hours each time to complete the process. Plaintiff Crespin faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

37. Plaintiff Barbara Lujan ("Plaintiff Lujan"), a resident of Pecos, New Mexico, was treated at Alta Vista Regional Hospital, affiliated with CHS, between 2011 and 2012. As part of the patient-admission process, Plaintiff B-Lujan was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Lujan's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Plaintiff Lujan faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

38. Plaintiff Lisa Maes ("Plaintiff Maes"), a resident of Las Vegas, New Mexico, was treated at Alta Vista Regional Hospital, affiliated with CHS, many times during the period 2006 to 2015. As part of the patient-admission process, Plaintiff Maes was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Maes' confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Plaintiff Maes faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

39. Plaintiff John Sanchez ("Plaintiff Sanchez"), a resident of Holman, New Mexico, was treated at Alta Vista Regional Hospital, affiliated with CHS, in 2011 and 2012. As part of the patient-admission process, Plaintiff Sanchez was required to provide CHS with his confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Sanchez' confidential patient data was misappropriated and exposed to identity thieves in and as result of the CHS data breach and he suffered cognizable injury thereby. Plaintiff Sanchez was prevented from filing his 2014 federal tax returns, as someone else using Plaintiff Sanchez' Social Security number had already filed a 2014 return in his name. Plaintiff Sanchez has paid his tax accounting firm, H&R Block, fees to help him deal with the tax return situation. To address the problems he encountered filing his 2014 taxes, Plaintiff Sanchez has spent a significant amount of time trying to rectify the situation with H&R Block and the IRS, and by monitoring all of his accounts. Plaintiff Sanchez faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of his confidential patient data, like all members of the proposed class.

40. Plaintiff Myrtle Keene ("Plaintiff Keene"), a resident of Warren, Ohio, treated with Dr. Michael Smith at an outpatient surgical center in Warren, Ohio affiliated with CHS, in 2014. As part of the patient-admission process, Plaintiff Keene was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Keene's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Plaintiff Keene faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

41. Plaintiff Betty Fowler ("Plaintiff Fowler"), a resident of Tulsa, Oklahoma, treated at a facility affiliated with CHS prior to the data breach. As part of the patient-admission process, Plaintiff Fowler was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Fowler's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Plaintiff Fowler faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

42. Plaintiff Karen Menke ("Plaintiff Menke"), a resident of Medford, Oregon, was treated at the Venice Regional Hospital, affiliated with CHS, in 2013. As part of the patient-admission process, Plaintiff Menke was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Menke's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury

thereby. Plaintiff Menke faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

43. Plaintiff Cynthia Horgan ("Plaintiff Horgan"), a resident of West Grove, Pennsylvania, was treated at Jennersville Hospital, affiliated with CHS, prior to the CHS data breach. As part of the patient-admission process, Plaintiff Horgan was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Horgan's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Plaintiff Horgan faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

44. Plaintiff William Lutz ("William Lutz"), a resident of Lafayette Hill, Pennsylvania, was treated at Northwest Internal Medicine, which is connected with Chestnut Hill Hospital, a CHS facility, during the period of the CHS data breach. As part of the patient-admission process, Plaintiff Lutz was required to provide CHS with his confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Lutz' confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and he suffered cognizable injury thereby. Since the CHS data breach, third parties have hacked into Plaintiff Lutz' email, changed his passwords repeatedly, and used Plaintiff's email account to identify his financial assets and credit accounts and have further used it to communicate with financial institutions and others to set up new accounts in Plaintiff Lutz' name. Plaintiff Lutz has experienced unauthorized charges on

his credit cards, withdraws from a hotel points account, and third parties have attempted to open at least two different foreign exchange accounts in Plaintiff Lutz' name. To address these activities, Plaintiff Lutz has spent a significant amount of time calling and corresponding with his email provider, credit card issuers, banks, financial institutions involved in foreign currency exchange, local police, the office of Social Security, Pay Pal, the Internal Revenue Service, credit reporting agencies, and Chex Systems. Plaintiff Lutz has also been in touch with elected officials, trying to regain control of his identity. In some instances, Plaintiff Lutz has expended his own funds to address these thefts. Plaintiff Lutz faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of his confidential patient data, like all members of the proposed class.

45. Plaintiff David Smith ("Plaintiff Smith"), a resident of New Castle, Pennsylvania, treated at a facility affiliated with CHS prior to the data breach. As part of the patient-admission process, Plaintiff Smith was required to provide CHS with his confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Smith's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and he suffered cognizable injury thereby. Plaintiff Smith faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of his confidential patient data, like all members of the proposed class.

46. Plaintiff Carolyn Pierce ("Plaintiff Pierce"), a resident of Chesterfield, South Carolina, was treated at Chesterfield General Hospital, affiliated with CHS, during the period 2000 to 2014. As part of the patient-admission process, Plaintiff Pierce was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance

with industry standards and as mandated by law. Plaintiff Burns' confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Plaintiff Pierce faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

47. Plaintiff Christopher Brown ("Plaintiff Brown"), a resident of Lexington, Tennessee, was treated at CHS affiliated hospitals from 2008 to 2014. As part of the patient-admission process, Plaintiff Brown was required to provide CHS with his confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Brown's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and he suffered a cognizable injury thereby. Since the CHS data breach, Plaintiff Brown has experienced unauthorized charges on his credit card, a cell phone was purchased in his name, and his credit score has plummeted. To address these activities, Plaintiff Brown has spent a minimum of forty hours dealing with the ramifications of the theft of his identity and he has spent $1,100 to purchase protection from a credit repair company. Plaintiff Brown faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of his confidential patient data, like all members of the proposed class.

48. Plaintiff Tara June Moore ("Plaintiff Moore"), a resident of Murfreesboro, Tennessee, was treated at CHS affiliated hospitals from 2000 to the present. As part of the patient-admission process, Plaintiff Moore was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Moore's confidential patient data was misappropriated and

exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Since the CHS data breach, Plaintiff Moore has experienced the unauthorized use of her bank account, unauthorized charges on her credit card, hacking of her personal email account, the fraudulent opening of new financial accounts in her name, and the unauthorized use of online payment services. To address these activities, Plaintiff Moore has spent significant time dealing with the ramifications of the theft of her identity. Plaintiff Moore faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

49. Plaintiff Juan Mendoza ("Plaintiff Mendoza"), a resident of Cypress, Texas, treated at a CHS facility prior to the time of the data breach. As part of the patient-admission process, Plaintiff Mendoza was required to provide CHS with his confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Mendoza's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and he suffered cognizable injury thereby. After receiving notice of the data breach, Plaintiff Mendoza purchased a subscription with LifeLock. Plaintiff Mendoza faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of his confidential patient data, like all members of the proposed class.

50. Plaintiff Brandon Mitchem ("Plaintiff Mitchem"), a resident of Falls Mills, Virginia, treated and continues to treat at Bluefield Internal Medicine, a CHS-affiliated medical center, from 2008 to the present. As part of the patient-admission process, Plaintiff Mitchem was required to provide CHS with his confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Mitchem's

confidential patient data was misappropriated and exposed to identity thieves in and as result of the CHS data breach and he suffered cognizable injury thereby. Plaintiff Mitchem faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of his confidential data, like all members of the proposed class.

51. Plaintiff Edward Adams ("Plaintiff Adams"), a resident of Oak Harbor, Washington, has treated at a medical facility, the Rockwood Eye Center (South), affiliated with CHS, since 1995. As part of the patient-admission process, Plaintiff Adams was required to provide CHS with his confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Adams' confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and he suffered cognizable injury thereby. Plaintiff Adams faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of his confidential patient data, like all members of the proposed class.

52. Plaintiff Melissa Harms ("Plaintiff Harms"), a resident of Otis Orchards, Washington, was treated at facilities in the Spokane Valley area of Washington affiliated with CHS prior to the CHS data breach. As part of the patient-admission process, Plaintiff Harms was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Harms' confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Plaintiff Harms faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of his confidential patient data, like all members of the proposed class.

53. Plaintiff Mary Glah ("Plaintiff Glah"), a resident of Bluefield, West Virginia, was treated at Bluefield Regional Medical Center and Bluefield Clinic Company, LLC, CHS affiliated hospitals, from 1990 to the present. As part of the patient-admission process, Plaintiff Glah was required to provide CHS with her confidential patient data, which CHS promised would be protected in accordance with industry standards and as mandated by law. Plaintiff Glah's confidential patient data was misappropriated and exposed to identity thieves in and as a result of the CHS data breach and she suffered cognizable injury thereby. Since the CHS data breach, Plaintiff Glah has experienced unauthorized use of her credit cards, and she has had to close several accounts to prevent further fraud. To address these activities, Plaintiff Glah has spent significant time dealing with the ramifications of the theft of her identity. Plaintiff Glah faces an ongoing, imminent, certainly impending threat of future additional harm from the theft of her confidential patient data, like all members of the proposed class.

54. Defendant Community Health Systems, Inc. is one of the nation's leading healthcare providers and touts itself as "one of the largest publicly-traded hospital companies in the United States and a leading operator of general acute care hospitals in communities across the country."[1] Through a network of affiliates, CHS owns or leases 199 hospitals in 29 states with approximately 30,000 licensed beds, and provides outpatient and physician services through a variety of facilities, including rehabilitation centers, urgent care centers, occupational medicine clinics, imaging centers, cancer centers, ambulatory surgery centers, and home health and hospice agencies.[2] According to CHS, through the management and operation of its network of affiliates, it is able to "provide standardization and centralization of operations across key

[1] *See* CHS Form 10-K at 1 (for the year ending Dec. 31, 2014).
[2] *Id.*

business areas."[3] CHS's "standardization and centralization initiative" encompasses nearly every aspect of its business, including "patient accounting and physician practice management."[4]

55. CHS Chief Executive Officer and Chairman of the Board Wayne T. Smith wrote in his 2014 Letter to Stockholders of CHS's "work to develop regional healthcare networks" and CHS's appreciation for "the outstanding physicians and caring employees in these hospitals" and "their active participation in our resolute commitment to deliver quality, compassionate, cost-effective care as we form a stronger, combined organization."[5] CHS CEO Smith also described CHS "deployed vast resources to improve clinical services and operational and financial performance."[6] Further, CEO Smith wrote, "I am most proud of the quality care we provide for patients" as he recounted CHS's "relentless focus on reducing the inherent risks of health-care delivery."[7] CHS CEO Smith also noted CHS's creation of eleven regional healthcare networks and CHS's investment in freestanding emergency rooms, diagnostic clinics, surgery centers, and multi-specialty group practices.[8] "Our ability to effectively deliver outpatient services already is evident in the hundreds of clinics, 63 ambulatory surgery centers, 41 urgent treatment centers, and 130 home health agencies we currently operate."[9]

56. CHS employs thousands of medical professionals. CHS CEO Smith wrote in his Letter to Investors that "more than 3,300 physicians have chosen to be employed with our organization."[10] He additionally wrote, "Our employees are valued partners in the care of millions of patients. We appreciate their skills and professionalism and see, daily, how their

[3] *Id.*
[4] *Id.* at 4.
[5] 2014 Annual Report to Stockholders, Community Health Systems, Inc., at 2.
[6] *Id.*
[7] *Id.*
[8] *Id.* at 3.
[9] *Id.*
[10] *Id.*

kindness brings comfort to those who are sick or hurting." CHS CEO also thanked CHS's "medical staffs and employees who dedicate themselves daily to the highest clinical and ethical standards."[11]

57. CHS is headquartered at 4000 Meridian Boulevard, Franklin, Tennessee 37067.

58. Defendant Community Health Systems Professional Services Corporation provides management, consulting, and information technology services to hospitals and health systems, as well as to certain clinics and physician practice operations.

59. Defendant CHPSC operates as a subsidiary of Defendant CHS, Inc.

60. CHRSC is headquartered at 4000 Meridian Boulevard, Franklin, Tennessee 37067.

JURISDICTION AND VENUE

61. This Court has original jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2). The amount in controversy in this action exceeds $5,000,000, exclusive of interest and costs, and there are more than 100 members of the classes defined below, the majority of whom reside in different states than Defendants.

62. Venue is proper in this Court pursuant to 28 U.S.C. § 1391, because Defendants regularly transact business in this District, and a substantial part of the events giving rise to this Complaint arose in this District.

FACTUAL BACKGROUND: THE DATA BREACH LANDSCAPE AND CHS'S FAILURES

63. The risks of data breaches in the healthcare industry have been known for a long time. As the federal Government Accounting Office ("GAO") noted in a 2005 report:

[11] *Id.*

> Since its creation, the SSN has evolved beyond its original intended purpose. This is significant, because these numbers, along with a name and birth date, are the three pieces of information most often sought by identity thieves. Once an SSN is obtained fraudulently, it can then be used as "breeder" information to create additional false identification documents, such as driver's licenses.[12]

64. In September of 2013, the Ponemon Institute issued a report entitled "2013 Report on Medical Identity Theft." Among the findings of the report were the following:

> **The number of medical identity theft victims increased**. The number of new cases over the past year is estimated at 313,000. This estimated increase in the base rate of identity theft victims climbed from .0068 to .0082, which represents a 19 percent increase over on year.
>
> **Medical identity theft can put victims' lives at risk**. The individuals in this study understand what medical identity theft is and have had personal experience with this crime either directly or through an immediate family member. However, 50 percent are not aware that medical identity theft can create inaccuracies in their permanent medical records.
>
> **Most medical identity theft victims lose trust and confidence in their healthcare provider following the loss of their medical credentials**. The most frequent medical consequence of a medical identity theft is that respondents lost trust and confidence in their healthcare provider (56 percent). This is an increase from 51 percent in last year's study.[13]

65. In February of 2014, the SANS Institute issued a "Healthcare Cyberthreat Report" in which it stated:

> Some 94 percent of medical institutions said their organizations have been victims of a cyberattack, according to the Ponemon Institute. Now, with the push to digitize all health care records, the emergence of HealthCare.gov and an outpouring of electronic protected health information (ePHI) being exchanged online, even more attack surfaces are being exposed in the healthcare field.
>
> A SANS examination of cyberthreat intelligence provided by Norse supports these statistics and conclusions, revealing exploited medical devices, conferencing systems, web servers, printers and edge security technologies all sending out malicious traffic from medical organizations. Some of these devices and

[12] U.S. GAO, *Social Security Numbers: More Could Be Done to Protect SSNs*, Report Number GAO-06-586T (Mar. 30, 2006), *available at* http://www.gao.gov/assets/120/113277.html. All websites were last visited on June 28, 2015 unless otherwise noted.

[13] *Available at* http://medidfraud.org/2013-survey-on-medical-identity-theft/.

> applications were openly exploitable (such as default admin passwords_ for many months before the breached organization recognized or repaired the breach.
>
> The intelligence data that SANS examined for development of this report was specific to the health care sector and was collected between September 2012 and October 2013. The data analyzed was alarming. It not only confirmed how vulnerable the industry and become, it also revealed how far behind industry-related cybersecurity strategies and controls have fallen.[14]

66. The Federal Bureau of Investigation's ("FBI") CyberDivision issued a "Private Industry Notification" on April 8, 2014, that cited the SANS report and Ponemon report and concluded that "the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs). The health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely."[15] The FBI stated further that:

> Health care security strategies and practices are poorly protected and ill-equipped to handle new cyber threats exposing patient medical records, billing and payment organizations, and intellectual property . . . The biggest vulnerability was the perception of IT healthcare professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise.[16]

67. Likewise, the California Attorney General issued a "Data Breach Report" in October of 2014. It observed as follows:

> In the health care sector, breaches affected more records than in other industry sectors, with the exception of retain since the two mega breaches of 2013. Many of the health care breaches reported to us are of a type that could be prevented by the strategic use of encryption. Unlike other industry sectors, where computer intrusions caused the majority of breaches, in healthcare 70 percent of breaches reported in the past two years were the result of stolen or lost hardware or digital media containing unencrypted personal information.

---

[14] *Available at* http://www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735.
[15] *Available at* http://www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf.
[16] *Id.*

> A recent study by the Poneon Institute reports that criminal attacks targeting the health care system are growing and that employees' use of unsecured portable devices is also increasing the risk of breach. The need to use encryption is a lesson that must be learned by the health care industry and we recommend that it be applied not only to laptops and portable media, but also to many computers in offices.

The report went on to note that on in three data breach victims in 2013 became identity theft victims in that same year, an increase from one in four in 2012.[17]

68. By early 2014, computer breaches had become rampant in the healthcare industry, a fact widely disseminate inside and outside the healthcare sector. For example:

- According to the Ponemon report, 63% of the healthcare organizations surveyed reported a data breach during the previous two years. The majority of these breaches resulted in the theft of data. In a March 2014 report, the institute stated that criminal attacks on healthcare companies have increased 100% since 2010.[18]

- An EMC2/RSA White Paper published in 2013 indicated that during the first half of 2013, more than two million healthcare records were compromised, constituting 31% of all reported data breaches.[19]

- According to the Identity Theft Resource Center, nearly half of all data breaches in 2014 took place in the healthcare sector, the largest single sector.[20]

- According to a recent analysis of data from the United State Department of Health & Human Services ("HHS") by the Washington Post's *Wonkblog*, the personal data of about 30.1 million people has been affected by 944 recorded "major" health data breaches (defined by HHS as one affecting at least 500 people) since federal reporting requirements under the 2009 economic stimulus package went into effect. This analysis did not include the CHS breach.[21]

---

[17] *Available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf.
[18] *See supra* note 13.
[19] *Available at* http://www.emc.com/collateral/white-papers/h12105-cybercrime-healthcare-industry-rsa-wp.pdf.
[20] Identity Theft Resource Center, *Identity Theft Resource Center Breach Report Hits Record High in 2014* (Jan. 12, 2015), http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html.
[21] Jason Millman, *Health Care Data Breaches Have Hit 30M Patients and Counting*, The Wash. Post (Aug. 19, 2014), http://www.washingtonpost.com/blogs/wonkblog/wp/2014/08/19/health-care-data-breaches-have-hit-30m-patients-and-counting/.

69. Several other studies have shown the healthcare industry to be one of the most affected by and least prepared to deal with hacking attempts. Despite the growing threat, the healthcare industry has been slow to implement improved security measures –slower than other industries handling sensitive information, such as the retail and financial sectors. For instance, the typical healthcare entity allocates only about two or three percent of its operating budget to its IT department, which retail and financial businesses devote more than 20 percent to IT. According to an annual security assessment conducted by the Healthcare Information and Management Systems Society, almost half of surveyed health systems said they spent three percent or less of their IT budgets on security.[22]

70. Thus, CHS was well aware of the very real threat of cyber-attacks when, in March 2014, the month before hackers infiltrated CHS and obtained the private information of millions of Defendants' patients, a Google researcher discovered the flaw that was then detected, but inexplicably was not corrected, in CHS's system, and led to a massive data extraction from CHS's computer network.[23] Days later, security firm Codenomicon independently discovered the same flaw.[24]

71. The existence of this software flaw—called the Heartbleed Vulnerability—was made public on April 7, 2014, and a simple patch to prevent hackers from using the vulnerability to access systems such as CHS's was issued the same day.[25] The flaw and its fix were widely

[22] *See* Healthcare Information and Management Systems Society, *6th Annual HIMSS Security Study* at 4 (Feb. 19, 2014), http://www.himss.org/files/2013_HIMSS_Security_Survey.pdf.
[23] Ben Grubb, *Heartbleed disclosure timeline: who knew what and when*, Sydney Morning Herald (Apr. 15, 2014), http://www.smh.com.au/it-pro/security-it/heartbleed-disclosure-timeline-who-knew-what-and-when-20140415-zqurk.html; Richard Neiva, *Heartbleed bug: What you need to know (FAQ)*, CNET (Apr. 11, 2014), http://www.cnet.com/news/heartbleed-bug-what-you-need-to-know-faq/.
[24] *Id.*
[25] *Hello, my name is Heartbleed*, *ITToday*,

publicized by national news shows, newspapers, online news organizations, and security industry experts.[26]

72. But CHS heeded none of the warnings or fixes. CHS failed to patch its systems, failed to change its security keys, and did not take even the simple step of changing system passwords.

73. Three days later, Juniper Networks, the company that manufactured the test server ("the Device") that hackers ultimately used to obtain CHS user credentials, issued security patches to fix the vulnerabilities that left the private data of Defendants' patients open to hackers.[27] The cyber security community also published and widely distributed procedures that companies were encouraged to follow in responding to Heartbleed. In fact, Codenomicon, the security company that discovered Heartbleed, immediately created "heartbleed.com" to educate the public about how to protect against the software flaw.[28] Again, CHS failed to apply the patch, or any other fixes, continuing to leave CHS's systems and the confidential data of its patients vulnerable.

74. Plaintiffs and the members of the proposed classes were required to provide their confidential patient data to Defendants in order to receive care. Plaintiffs and members of the

---

http://www.ittoday.info/Articles/heartbleed_infographic.pdf.

[26] *See, e.g.*, Steve Lohr, *Heartbleed Security Flaw Emphasizes the Need to Change Passwords*, N.Y. Times (Apr. 8, 2014), http://bits.blogs.nytimes.com/2014/04/08/security-flaw-emphasizes-the-need-to-change-passwords/; Heather Kelly, *The 'Heartbleed' security flaw that affects most of the Internet*, CNN (Apr. 9, 2014), http://www.cnn.com/2014/04/08/tech/web/heartbleed-openssl/; Danny Yardon, *After Heartbleed Bug, a Race to Plug Internet Hole*, WSJ (Apr. 9, 2014), http://www.wsj.com/articles/SB10001424052702303873604579491350251315132; *What you need to know about the Heartbleed bug*, Fox News (Apr. 10, 2014), http://www.foxnews.com/tech/2014/04/10/what-need-to-know-about-heartbleed-bug/.

[27] Morris Stemp, *Failure to Perform Upgrades Caused Breach at Community Health Systems*, stempsystems (Sept. 9, 2014), http://stempsystems.com/failure-to-perform-upgrades-caused-community-health-systems-breach/; *The Heartbleed Bug*, Heartbleed.com (last visited June 22, 2015).

[28] Neiva, *supra*.

proposed classes paid for services provided by Defendants' health care network, and part of that payment was for the protection and security of their confidential patient data.

75. Defendants came into possession of the confidential patient data for 4.5 million CHS patients, which was then accessed without Plaintiffs' authorization, and which has been used, or certainly will be used, to steal Plaintiffs' identities and subject them to fraud and abuse.

76. CHS made it easy for hackers to steal the most private information of its patients. According to David Kennedy, CEO at TrustedSec, immediate implementation of the Heartbleed fix would have ***thwarted*** the Data Breach.[29]

77. Vincent Berk, the CEO of the data security company Flow/Traq, and a Ph.D. in computer science, noted that competent and caring security professionals would have taken immediate remediation steps.[30] He also stated that CHS's failure to patch its networks and change security keys and passwords meant, "CHS didn't care or they're just not qualified."[31]

78. Cyber security commentators have stated that the consequences of CHS's inaction were ***"utterly foreseeable"*** and ***"could have been easily anticipated and guarded against."***[32]

79. Three months after the Heartbleed Vulnerability was announced, and simple fixes were offered, in July 2014, CHS discovered the Data Breach that it had allowed to occur.

---

[29] Danielle Walker, *Community Health Systems attackers exploited Heartbleed bug for access, firm says*, SCMagazine (Aug. 20, 2014), http://www.scmagazine.com/community-health-systems-attackers-exploited-heartbleed-bug-for-access-firm-says/article/367249/.

[30] Sara Peters, *Heartbleed Not Only Reason For Health Systems Breach*, Dark Reading (Aug. 20, 2014), http://www.darkreading.com/heartbleed-not-only-reason-for-health-systems-breach/d/d-id/1298157.

[31] *Id.*

[32] Paula Knippa, *What Healthcare Can Learn From CHS Data Breach*, InformationWeek (Nov. 25, 2014), http://www.informationweek.com/healthcare/security-and-privacy/what-healthcare-can-learn-from-chs-data-breach/a/d-id/1317696.

80. But CHS did not promptly notify its patients that their confidential patient data had been taken. In fact, CHS waited until August 2014, the following month, to inform Plaintiffs and the members of the proposed classes that hackers had stolen their confidential patient data.

81. Within days of CHS disclosing its Data Breach, experts reported that hackers accessed the CHS network by exploiting the Heartbeat Vulnerability, an unsophisticated flaw in the OpenSSL software library that is easily remedied.[33] In fact, preventing access via Heartbleed requires just two steps. First, a user and/or service provider must install and employ the updated version of OpenSSL, released the same day the Heartbleed Vulnerability was publicly disclosed, to its servers.[34] Second, the encryption keys and corporate passwords that may have been compromised must be updated and changed to prevent hackers from impersonating users and/or administrators through stolen credentials.[35]

---

[33] OpenSSL software provides security and privacy for Internet communication occurring by email, instant messaging, and virtual private networks ("VPN"). *The Heartbleed Bug*, Heartbleed.com (last visited June 22, 2015). (A VPN is a network that uses public wires—in this case the Internet—to connect a private network, such as the internal network of a company.) The Heartbleed Vulnerability is a relatively crude coding error in the OpenSSL software. When two servers exchange information, they send data back and forth to ensure each is still participating in the transaction, known as heartbeats. This heartbeat exchange includes data of various sizes, and Heartbleed allows a hacker to represent a data size of 64kb (the maximum allowed), which triggers a response of 64kb of data to the hacker. But the return heartbeat to the hacker consists of random bits of data off the server's memory, which allows hackers to randomly compile large amounts of information from a server's memory. Once the information is compiled via the Heartbleed Vulnerability, hackers use other technology to sift through the randomly stolen information and identify, among other things, security keys, usernames, and passwords. *See* Eric Limer, *How Heartbleed Works: The Code Behind the Internet's Security Nightmare*, Gizmodo (Apr. 9 , 2015), http://gizmodo.com/how-heartbleed-works-the-code-behind-the-internets-se-1561341209; Neil J. Rubenking, *Heartbleed: How It Works*, SecurityWatch (Apr. 10, 2014), http://securitywatch.pcmag.com/hacking/322533-heartbleed-how-it-works.

[34] Nicole Perlroth, *Experts Find a Door Ajar in an Internet Security Method Thought Safe*, N.Y. Times (Apr. 8, 2014); *Hello, my name is Heartbleed, ITToday*, http://www.ittoday.info/Articles/heartbleed_infographic.pdf.

[35] Perlroth, *supra*.

82. But CHS did not take either of these rudimentary steps to protect its system, and the Heartbleed Vulnerability allowed hackers to target the network flaw to steal user credentials from the memory of a test server, the Device, manufactured by Juniper Networks.[36] CHS's use of this test server further opened the door to the devastating Data Breach. Because the CHS Device was a test server, it was never intended to be connected to the Internet.[37] As such, the security features and updates normally installed and relied on to secure sensitive data did not exist on the Device.[38] Some commentators have stated that by storing sensitive credentials on a test server it was as if "CHS left the lights on and a note on the door, saying, 'Hey, come on in. The key is under the doormat!'"[39]

83. After the hackers stole user credentials, they used CHS's VPN to gain remote access to the CHS network.[40] The stolen credentials allowed the hackers to freely navigate CHS's internal systems. The hackers then worked their way through CHS's network until they removed the 4.5 million customer records.[41]

84. CHS further set the stage for a massive data breach by failing to monitor its network. Extracting 4.5 million customer records did not occur overnight and took some time to achieve. The removal of such a large data set over a long period of time should have raised red flags and the fact that it did not suggests that CHS failed to monitor whether data left its network.[42]

---

[36] Stemp, *supra*.
[37] Knippa, *supra*.
[38] *Id.*
[39] *Id.*
[40] Davek, *CHS Hacked via Heartbleed Vulnerability*, TrustedSec (Aug. 19, 2014) https://www.trustedsec.com/august-2014/chs-hacked-heartbleed-exclusive-trustedsec/.
[41] *Id.*
[42] Peters, *supra*.

85. Vincent Berk stated that CHS's failure to monitor its outgoing network activity was "downright embarrassing . . . Nobody was watching. Nobody was stopping it."[43] In addition to CHS's failure to monitor its outgoing network activity, the fact that CHS did not recognize that a client in China[44] was connecting to its VPN network with the credentials of an affiliated-doctor who usually works from home in Alabama, suggests that CHS wasn't even monitoring incoming network activity.[45]

86. CHS's failure to monitor its network activity may be more alarming than its failure to properly respond to Heartbleed. Credentials can be stolen in a number of ways separate from Heartbleed. For this reason, it is imperative that companies properly monitor their systems and the behavior of their users. The banking industry has already done just that:

banks now routinely monitor for inconsistencies in customers' purchasing activities. For example, if an expensive purchase is made at a point-of-sale machine in Italy, when the legitimate customer is still buying groceries as usual at home in Alabama, the account may be flagged and frozen.[46]

87. Lookingglass, a leading company in cyber intelligence management, independently evaluated CHS's computer network and confirmed that CHS's systems were not adequately protected. Lookingglass found that 10 CHS IP addresses were linked to "various bots and blacklists" known for data exfiltration, banking credential theft, and more.[47] According to Lookingglass, multiple threat indicators were associated with the questionable IP addresses, indicating they are gateways with multiple hosts behind them with a high likelihood that the

---

[43] *Id.*
[44] In its 8-K and 10-K, CHS claimed the attack emanated from China.
[45] Pagliery, *supra*.
[46] Peters, *supra*.
[47] Jason Lewis, *Looking Glass* (Aug. 21, 2014), https://lgscout.com/where-there-are-breaches-there-are-infections/.

hosts can also access CHS's VPN.[48] Additionally, the Lookingglass assessment uncovered active infections via Conficker, a virus discovered and patched in 2008, which suggests that CHS's systems have gone unpatched for years.[49] Based on CHS's abysmal security practices, Lookingglass stated "[i]f an advance[d] nation-state [like China] penetrated [CHS's] network, they probably didn't have to work very hard to gain a foothold."[50]

88. CHS also failed to effectively segment its customer database.[51] No single hospital, affiliated-physician's office, or care center had 4.5 million patient records. As such, the stolen credentials allowed hackers to either maneuver across databases and remove records wherever in CHS's system they were located. CHS improperly stored the records and configured its network in such a way as to allow free roaming access to CHS network users.

89. On August 18, 2014, Defendant CHS, Inc. filed a Form 8-K with the United States Securities and Exchange Commission ("SEC") that provided the first notification of the Data Breach. The filing stated:

> In July 2014, Community Health Systems, Inc. (the "Company") confirmed that its computer network was the target of an external, criminal cyber-attack that the Company believes occurred in April and June, 2014. The Company and its forensic expert, Mandiant (a FireEye Company), believe the attacker was an "Advanced Persistent Threat" group originating from China who used highly sophisticated malware and technology to attack the Company's systems. The attacker was able to bypass the Company's security measures and successfully copy and transfer certain data outside the Company. Since first learning of this attack, the Company has worked closely with federal law enforcement authorities in connection with their investigation and possible prosecution of those determined to be responsible for this attack. The Company also engaged Mandiant, who has conducted a thorough investigation of this incident and is advising the Company regarding remediation efforts. Immediately prior to the filing of this Report, the Company completed eradication of the malware from its systems and finalized the implementation of other remediation efforts that are

[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] Peters, *supra*.

> designed to protect against future intrusions of this type. The Company has been informed by federal authorities and Mandiant that this intruder has typically sought valuable intellectual property, such as medical device and equipment development data. However, in this instance the data transferred was non-medical patient identification data related to the Company's physician practice operations and affected approximately 4.5 million individuals who, in the last five years, were referred for or received services from physicians affiliated with the Company. The Company has confirmed that this data did not include patient credit card, medical or clinical information; the data is, however, considered protected under the Health Insurance Portability and Accountability Act ("HIPAA") because it includes patient names, addresses, birthdates, telephone numbers and social security numbers. The Company is providing appropriate notification to affected patients and regulatory agencies as required by federal and state law. The Company will also be offering identity theft protection services to individuals affected by this attack. The Company carries cyber/privacy liability insurance to protect it against certain losses related to matters of this nature. While this matter may result in remediation expenses, regulatory inquiries, litigation and other liabilities, at this time, the Company does not believe this incident will have a material adverse effect on its business or financial results.[52]

90. On August 19, 2014, Defendant CHSPSC published a "Data Breach Notification" on their public website. The Notification stated:

> On behalf of Community Health Systems Professional Services Corporation ("CHSPSC"), I want to express sincere regret to the patients of affiliated physician practices and clinics whose data was accessed in a foreign-based cyber-attack of our computer network. We value the trust you have placed in us for your care and it is our priority to ensure those who were affected by this attack are notified about the breach and have their questions answered. If you were affected by the data breach, you will receive a letter with more information and a toll-free number to call to learn about the free identity theft protection offered to affected patients. The following notice contains more details about the breach, measures we are taking to notify you, and how we are improving the way we protect health your information [sic].
>
> In July 2014, Community Health Systems Professional Services Corporation ("CHSPSC") confirmed its computer network was the target of an external criminal cyber-attack in April and June 2014. CHSPSC, a Tennessee company, provides management, consulting, and information technology services to certain clinics and hospital-based physicians in this area.

[52] Defendants' August 18, 2014, SEC filing is available at http://www.chs.net/investor-relations/sec-fillings/.

> CHSPSC believes the attacker was an "Advanced Persistent Threat" group originating from China, which used highly sophisticated malware technology to attack CHSPSC's systems. The intruder was able to bypass the company's security measures and successfully copy and transfer some data existing on CHSPSC's systems.
>
> Since first discovering the attack, CHSPSC has worked closely with federal law enforcement authorities in connection with their investigation of the matter. CHSPSC also engaged an outside forensic expert to conduct a thorough investigation and remediation of this incident. CHSPSC has implemented efforts designed to protect against future intrusions. These efforts include implementing additional audit and surveillance technology to detect unauthorized intrusions, adopting advanced encryption technologies, and requiring users to change their access passwords.
>
> The majority of patients of clinics and hospital-based physicians affiliated with CHSPSC were not affected by this breach. Individuals whose information was taken in this cyber-attack will be mailed a letter informing them about the data breach and how to enroll in free identity theft protection and credit monitoring services. The data taken includes patients' names, addresses, birthdates, social security numbers, and, in some cases, telephone numbers, and the names of employers or guarantors. However, to the best of CHSPSC's knowledge, NO credit card information was taken and NO medical or clinical information was taken. CHSPSC recommends that you remain vigilant for incidents of fraud and identity theft by reviewing your credit report and accounts for unauthorized activity.
>
> Anyone with questions or concerns about this cyber-attack may contact 1-855-205-6951 toll-free beginning Wednesday, August 20, 2014, at 8:00 a.m. central time. For information on preventing identity theft or to report suspicious activity, contact the Federal Trade Commission at 1-877-438-4338 or get free information at www.ftc.gov.[53]

91. As noted above, Defendants did not send Plaintiffs correspondence notifying them of the Data Breach until August 29, 2014.

92. All Plaintiffs and members of the proposed classes have suffered monetary damages and economic loss by overpaying for CHS-provided health care that was to include

[53] Defendants' August 19, 2014, Data Breach Notification was originally posted to http://www.chs.net/ media-notice-august-19-2014/. The page has been taken down, but an archived version is available at https://web.archive.org/web/20140823062745/http://www.chs.net/media-notice-august-19-2014.

appropriate data security, but ultimately did not include such security. Additionally, Plaintiffs and members of the proposed classes were harmed by having their confidential patient data misappropriated and made available to identity thieves. Many have suffered identity theft, fraud, and abuse, due to having their confidential patient data sold on the Internet black market resulting in monetary damages and economic loss, including but not limited to: unauthorized charges on bank and credit cards; fraudulently opened cards or accounts; emails hacked; impersonation by hackers with government agencies, credit card companies, and retailers; medical information stolen; cell phones and checking accounts hacked; fraudulent online payments; compromised credit scores; and fraudulent tax returns filed. All are at an increased and certain risk of becoming victims of identity theft crimes, fraud, and abuse due to having confidential patient data sold on the Internet black market (which will result in the same aforementioned monetary damages and economic loss), and all have been forced to spend considerable time and money to investigate and mitigate the imminent risk of harm from identity theft, fraud, and abuse as a result of Defendants' conduct, including, but not limited to: detecting and preventing identity theft and unauthorized use of financial and/or medical information; monitoring accounts for fraudulent charges; canceling and obtaining reissued credit cards; dealing with the IRS and other government agencies; purchasing credit monitoring and identity theft protection services and insurance.

LEGAL BACKGROUND: REQUIREMENTS FOR DATA PRIVACY AND CHS'S PROMISES TO PLAINTIFFS

93. The confidential patient data that was copied and transferred from Defendants' computer systems is considered protected "patient identification data" under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 29 U.S.C.A. §§ 1181 *et seq.*

because it includes patient names, addresses, birthdates, telephone numbers and Social Security numbers.

94. HIPAA required Defendants to "reasonably protect" the copied data from "any intentional or unintentional use or disclosure." 45 C.F.R. § 164.530(c)(1)(2)(i). Federal regulations also required Defendants to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." *Id.* at § 164.530(c)(1).

95. Defendants violated HIPAA by failing to maintain the confidentiality of Plaintiffs' and the proposed class members' protected patient identification data.

96. Defendants failed to safeguard and prevent vulnerabilities from being taken advantage of in their computer systems.

97. As a result of Defendants' failure to safeguard and prevent vulnerabilities from being taken advantage of in their computer systems, unauthorized third parties were able to bypass Defendants' inadequate security measures and successfully copy and transfer the confidential patient data of Plaintiffs and the members of the proposed classes.

98. The 2013 Identity Fraud Report released by Javelin Strategy & Research reports that in 2012 identity fraud incidents increased by more than one million victims and hackers stole nearly $21 billion. The study found 12.6 million victims of identity fraud in the United States in the past year, which equates to 1 victim every 3 seconds. The report also found that nearly 1 in 4 data breach letter recipients became a victim of identity fraud, with breaches involving Social Security numbers to be the most damaging.

99. To assist companies in protecting the security of sensitive personal and financial information, the Federal Trade Commission ("FTC") has issued a publication entitled

"Protecting Personal Information: A Guide for Business" (the "FTC Report"). In this publication, the FTC provides guidelines for businesses on how to develop a "sound data security plan" to protect against crimes of identity theft.

100. To protect the personal sensitive information in their files, the FTC Report instructs businesses to follow the following guidelines:

a) Keep inventory of all computers and laptops where the company stores sensitive data;

b) Do not collect personal information if there is no legitimate business need. If there is a legitimate business need, only keep the information as long as necessary;

c) Use Social Security numbers only for required and lawful purposes and do not store these numbers unnecessarily, such as for an employee or customer identification number;

d) Encrypt the personal information, particularly if the sensitive information is shipped to outside carriers or contractors. In addition, the business should keep an inventory of all the information it ships;

e) Do not store sensitive computer data on any computer with an Internet connection or access unless it is essential for conducting the business;

f) Control access to sensitive information by requiring that employees use "strong" passwords; and

g) Implement information disposal practices that are reasonable and appropriate to prevent unauthorized access to personally identifying information.

101. Defendants violated federal guidelines and failed to meet current data security industry standards by failing to ensure adequate security over Plaintiffs' and the proposed class members' confidential patient data and by failing to retain Plaintiffs' and the proposed class members' confidential patient data in a secure and safe manner.

102. By way of illustration and without limitation, on information and belief, Defendants failed to properly encrypt data, failed to establish adequate firewalls to handle a server intrusion contingency, and failed to implement adequate authentication protocol to protect the confidential information contained in its computer network.

103. On information and belief, the Data Breach also resulted from Defendants' pattern of un-patched systems and inadequate vulnerability management.

104. Defendants have assumed the duty to protect the confidential patient data of Plaintiffs and the members of the proposed classes.

105. Through its Notice of Privacy Practices (which is communicated to all patients), CHS represented that it would protect its patients' confidential patient data and keep it confidential. For instance, the Notice of Privacy Practices states in relevant part:

> "We understand that medical information about you and your health care is personal. We are committed to protecting medical information about you. A record is created of the care and services you receive at this facility. This record is needed to provide the necessary care and to comply with legal requirements."[54]
> * * * *
>
> "This notice applies to all of the records of your care generated by the facility . . . This notice will tell about the ways in which the facility may use and disclose medical information about you. Also described are your rights and certain obligations we have regarding the use and disclosure of medical information. The law requires the facility to: [m]ake sure that medical information that identifies you is kept private; [i]nform you of our legal duties and privacy practices with

[54] See Community Health's Notice of Privacy Practices, http://webapps.chs.net/HIPPA/(last visited Aug. 26, 2014)

> respect to medical information about you; and [f]ollow the terms of the notice that is currently in effect . . . . "[55]

106. Similarly, Defendants have published a "Code of Conduct," which contains a "Statement of Beliefs," which provides, in relevant part, as follows: "We have adopted the following Statement of Beliefs that summarizes the commitments of the organization's constituents ***to our patients***, colleagues, physicians, and the communities served . . . [W]e are dedicated to compliance with all federal, state, and local laws, rules, and regulations, ***including privacy and security of patient health information***."[56]

107. Further, the provisions of Defendants' Code of Conduct concerning the "Confidentiality of Patient Information" provide that:

> ***When a patient enters a CHS affiliated facility, a large amount of personal, medical, and insurance data is collected and used to satisfy information needs including the ability to make decisions about a patient's care. We consider patient information highly confidential.*** Colleagues are expected to take care to protect the privacy of individually identifiable health information at all times. All of the facilities within the organization have specific policies describing patient confidentiality and release of information rules that conform to federal, state, and local laws governing the release or disclosure of health information.[57]

108. Moreover, through their affiliates, Defendants have published patient resources regarding "Patient Rights & Responsibilities" and "HIPAA Compliance." By way of example, on its public website, Brandywine Hospital, one of Defendants' affiliated hospitals, assures patients, such as Plaintiffs and the members of the proposed classes, that they have the right to "[p]ersonal privacy" and "privacy of your health information."[58]

---

[55] *Id*.
[56] http://www.chs.net/wp-content/uploads/PDF/2014%20Code%20of%20Conduct.pdf (last visited June 16, 2015)
[57] *Id*. at 10 (emphasis added).
[58] *See* http://www.brandywine hospital.com/brandywinehospital/patientrightsandresponsibilities.aspx (last accessed June 16, 2015).

109. Brandywine Hospital further assures patients, such as Plaintiffs and the members of the proposed classes, of its "Pledge Regarding Medical Information," stating that "[w]e understand that medical information about you and your health care is personal. We are committed to protecting medical information about you."[59]

110. A portion of the consideration paid for health care by Plaintiffs and the members of the proposed classes was accepted by Defendants and was allocated to protecting and securing Plaintiffs' and the proposed class members' confidential patient data and ensuring HIPAA compliance. This allocation was made for the purpose of offering patients and consumers, such as Plaintiffs and the members of the proposed classes, added value to the healthcare services provided.

CLASS ACTION ALLEGATIONS

A. The National Class

111. Pursuant to Fed. R. Civ. P. 23, Plaintiffs assert their common law claims for breach of contract (Count I), breach of implied contract (Count II), unjust enrichment (Count III), negligence (Count IV), negligence *per se* (Count V), bailment (Count VI), wantonness (Count XI) and their federal statutory claims under the Fair Credit Reporting Act (Counts VII and VIII), on behalf of a nationwide class, defined as follows:

> All persons in the United States whose patient data was contained in or on Defendants' computer network and whose patient data was misappropriated as a result of the breach of Defendants' computer network, as announced by Defendants on or about August 18, 2014 ("National Class").

[59] https://web.archive.org/web/20140428095159/http://www.brandywinehospital.com/Brandywine-Hospital/hipaa1.aspx (last visited June 25, 2016)

112. As alleged herein, Defendants are headquartered in Tennessee, maintain their primary data center in Tennessee, and the employees charged with making decisions concerning data security are based in Tennessee. Defendants' conduct resulting in the Data Breach took place exclusively, or primarily, in Tennessee. Defendants, being headquartered in Tennessee, would reasonably expect to be bound by the common law of Tennessee. And finally, the injuries resulting from the data breach arose exclusively, or primarily, in Tennessee, where the information was misappropriated. Accordingly, applying Tennessee law to the common law claims of the National Class is appropriate.

B. The Alternate State Specific Classes

113. Pursuant to Fed. R. Civ. P. 23, and in the alternative to the common law claims asserted on behalf of the National Class, Plaintiffs assert their common claims for breach of contract (Count I), breach of implied contract (Count II), unjust enrichment (Count III), negligence (Count IV), negligence *per se* (Count V), bailment (Count VI), and wantonness (Count XI) under the laws of the individual states where Defendants maintained treatment facilities, and on behalf of separate statewide classes, defined as follows:

> All individuals who received treatment at a facility of Defendants in [name of State] whose patient data was contained in or on Defendants' computer network and whose patient data was misappropriated as a result of the breach of Defendants' computer network, as announced by Defendants on or about August 18, 2014 ("Alternate State Specific Classes").

C. State Statutory Classes

114. Pursuant to Fed. R. Civ. P. 23, Plaintiffs assert their claims that Defendants violated state consumer protection statutes (Count IX) and state data breach notification laws (Count X) on behalf of separate statewide classes, defined as follows:

> All residents of [name of State] whose patient data was contained in or on Defendants' computer network and whose patient data was misappropriated as a result of the breach of Defendants' computer network, as announced by Defendants on or about August 18, 2014 ("State Statutory Classes").

115. Plaintiffs assert the state consumer protection law claims (Count IX) under the listed consumer protection laws of: Arizona, Arkansas, Florida, Indiana, Illinois, Kentucky, New Mexico, Ohio, Oklahoma, Oregon, Missouri, Nebraska, New Jersey, Pennsylvania, Texas, Washington, and West Virginia.

116. Plaintiffs assert the state data breach notification law claims (Count X) on behalf of separate statewide classes in and under the respective data breach statutes of the States of: Georgia, Illinois, Kentucky, Louisiana, New Jersey, Oregon, South Carolina, Tennessee, Virginia, and Washington.

D. The Classes Meet the Criteria of Rule 23

117. Plaintiffs are members of the classes they seek to represent.

118. Excluded from each of the above classes are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

119. Each of the proposed classes meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

120. **Numerosity.** The classes are so numerous that joinder of all members is impracticable, as approximately four and one-half (4.5) million individuals' confidential patient data has been compromised.

121. **Commonality.** There are questions of law and fact common to all members of the classes, the answers to which will advance the resolution of the claims of the class members and that include, without limitation:

(i) Whether Defendants failed to provide adequate security and/or protection for their computer systems containing Plaintiffs' and the proposed class members' confidential patient data;

(ii) Whether Defendants owed a legal and/or contractual duty to Plaintiffs and the proposed class members to protect their confidential patient data and whether Defendants breached this duty;

(iii) Whether the conduct of Defendants resulted in the unauthorized breach of their computer systems containing Plaintiffs' and the proposed class members' confidential patient data;

(iv) Whether Plaintiffs and the proposed class members have been injured by Defendants' conduct;

(v) Whether Plaintiffs and class members are at an increased risk of identity theft as a result of Defendants' failure to protect Plaintiffs' and the proposed class members' confidential patient data;

(vi) Whether Defendants were negligent;

(vii) Whether Defendants breached their contract with Plaintiffs and the proposed class members;

(viii) Whether Plaintiffs and the proposed class members are entitled to injunctive relief; and

(ix) Whether Plaintiffs and the proposed class members are entitled to damages, and the measure of such damages.

122. **Typicality.** Plaintiffs' claims are typical of the claims of all members of the classes. Specifically, Plaintiffs' and class members' claims arise from Defendants' failure to install and maintain reasonable security measures, to implement appropriate policies, and to protect Plaintiffs' and class members' confidential patient data.

123. **Adequacy.** Plaintiffs are adequate representatives of the proposed classes because their interests do not conflict with the interests of the class members they seek to represent. Plaintiffs' counsel are very experienced in litigating consumer class actions and complex commercial disputes, and include lawyers who have litigated other similarly massive data breach cases.

124. **Superiority.** A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Defendants. Even if it were economically feasible, requiring millions of injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

125. **Predominance.** Common questions of law and fact predominate over individualized questions. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy.

126. Prosecuting separate actions by individual class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Defendants.

127. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). Defendants have acted or have refused to act on grounds generally applicable to the classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the classes.

128. The members of the classes are individuals who were referred for or received services from Defendants. As such, the members of the classes are readily ascertainable, as they can be identified by records maintained by Defendants. Notice can be provided by means permissible under Rule 23.

COUNT I
BREACH OF CONTRACT
(On behalf of the National Class and the Alternate State Specific Classes)

129. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein.

130. Plaintiffs and the proposed class members entered into contracts with Defendants for the provision of healthcare services. As a material term of such contracts, Defendants promised to comply with the requirements of HIPAA and to act reasonably to protect Plaintiffs and the proposed class members' confidential patient data.

131. Plaintiffs and the proposed class members paid money to Defendants in exchange for their promise to provide healthcare services, including compliance with HIPAA and the industry standards for protecting confidential patient data.

132. In the contracts and in Defendants' patients' rights and privacy notices, the Defendants promised to comply with HIPAA and its implementing regulations and only to

disclose Plaintiffs' and the proposed class members' patient identification information, which is part of the confidential patient data taken in the Data Breach, when required to do so by federal and/or state law, and to safeguard and protect Plaintiffs' and the proposed class members' confidential patient data from being compromised and/or stolen.

133. Plaintiffs and the proposed class members fully performed their obligations under the contracts.

134. Defendants did not safeguard or protect Plaintiffs' and the proposed class members' confidential patient data from being accessed, compromised, and/or stolen. Defendants did not maintain sufficient security measures and procedures to prevent unauthorized access to Plaintiffs' and the proposed class members' confidential patient data. Defendants did not comply with HIPAA or the industry standards for the protection of confidential patient data.

135. Because Defendants failed to safeguard and/or protect Plaintiffs' and the proposed class members' confidential patient data from being compromised or stolen, and failed to comply with HIPAA and the industry standards for the protection of such information, Defendants breached their contracts with Plaintiffs and the proposed class members.

136. Defendants' failure to fulfill their contractual obligation to protect confidential patient data resulted in the Plaintiffs and the proposed class members receiving healthcare services of less value than what was promised, i.e., healthcare services that included adequate protection of confidential patient data. Accordingly, Plaintiffs and the proposed class members did not receive the full benefit of their bargain.

137. Plaintiffs and the proposed class members have suffered and will continue to suffer damages as the result of Defendants' breach, including the monetary difference between the amount paid for healthcare services as promised (which were promised to include adequate

and HIPAA-compliant data protection) and the healthcare services actually provided by Defendants (which did not include adequate and/or HIPAA-compliant data protection).

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of the National Class and the Alternate State Specific Classes)

138. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein, except for the allegations in Count I (Breach of Contract), and bring this count in the alternative to Count I to the extent that an express contract is found not to exist between Defendants and Plaintiffs and the members of the proposed class.

139. As a necessary prerequisite to receiving healthcare treatment from Defendants, Plaintiffs and the proposed members of the class provided confidential patient data to Defendants.

140. Plaintiff and the proposed members of the class also disclosed such information for the benefit of Defendants.

141. The provision of confidential patient data by Plaintiff and the proposed members of the class, and Defendants' acceptance of such information, created an implied contract whereby Defendant had a duty to safeguard and protect the information of Plaintiff and the proposed members of the class, consistent with HIPAA and industry standards for confidential patient data protection.

142. Defendants did not safeguard or protect Plaintiffs' and the proposed class members' confidential patient data from being accessed, compromised, and/or stolen. Defendants did not maintain sufficient security measures and procedures to prevent unauthorized access to Plaintiffs' and the proposed class members' confidential patient data. Defendants did not comply with HIPAA or the industry standards for the protection of confidential patient data.

143. Because Defendants failed to safeguard and/or protect Plaintiffs' and the proposed class members' confidential patient data from being compromised or stolen, and failed to comply with HIPAA and the industry standards for the protection of such information, Defendants breached their implied contracts with Plaintiffs and the proposed class members.

144. Defendants' failure to fulfill their implied contractual obligation to protect confidential patient data resulted in the Plaintiffs and the proposed class members receiving healthcare services of less value than what was promised, i.e., healthcare services that included adequate protection of confidential patient data. Accordingly, Plaintiffs and the proposed class members did not receive the full benefit of their bargain.

145. Plaintiffs and the proposed class members have suffered and will continue to suffer damages as the result of Defendants' breach, including the monetary difference between the amount paid for healthcare services as promised (which were promised to include adequate and HIPAA-compliant data protection) and the healthcare services actually provided by Defendants (which did not include adequate and/or HIPAA-compliant data protection).

COUNT III
UNJUST ENRICHMENT
(On behalf of the National Class and the Alternate State Specific Classes)

146. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein, except for the allegations in Count I (Breach of Contract) and Count II (Breach of Implied Contract), and bring this count in the alternative to Count I and Count II to the extent that neither an express or implied contract is found to exist between Defendants and Plaintiffs and the members of the proposed class, in which case Plaintiffs and the members of the proposed class will have exhausted all other remedies against Defendants.

147. Defendants received payment from Plaintiffs, the National Class and the Alternate State Specific Classes to perform services that included protecting Plaintiffs' and the proposed class members' confidential patient data.

148. Defendants did not protect Plaintiffs' and the proposed class members' confidential patient data, but retained Plaintiffs' and the proposed class members' payments.

149. Defendants retained the benefits of Plaintiffs' and the proposed class members' payments under circumstances which rendered it inequitable and unjust for Defendants to retain such benefits without paying for their value.

150. Defendants have knowledge of said benefits.

151. Plaintiffs and the members of the National Class and the Alternate State Specific Classes are entitled to recover damages in an amount to be proven at trial.

152. For reasons set forth in detail elsewhere herein, Tennessee common law applies to the unjust enrichment claim of the National Class. However, if the National Class is not certified, the unjust enrichment claims of the Alternate State Specific Classes would be governed by the law of each state in which such state specific claims are brought.

COUNT IV
NEGLIGENCE
(On behalf of the National Class and the Alternate State Specific Classes)

153. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein.

154. Defendants owed – and continue to owe – a duty to Plaintiffs, the National Class and the Alternate State Specific Classes to use reasonable care in safeguarding confidential patient data from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty arises from several sources, including but not limited to the sources described

below, and is independent of any duty Defendants owed as a result of their contractual obligations. This confidential patient data includes but is not limited to patient names, addresses, birthdates, telephone numbers, Social Security numbers, and other personal information.

155. Defendants have a common law duty to prevent foreseeable risk of harm to others, including Plaintiffs, the National Class and the Alternate State Specific Classes. Defendants' duty includes, among other things, designing, maintaining, and testing their security systems to ensure that Plaintiffs' and the proposed class members' confidential patient data is adequately secured and protected and to implement processes that will detect a breach of their security systems in a timely manner.

156. As patients of Defendants' healthcare network, Plaintiffs the members of the proposed classes are part of a well-defined, foreseeable, finite and discernable group which was well-known and identifiable to Defendants before their conduct caused the harm at issue.

157. It was foreseeable that Defendants' failure to use reasonable measures to protect confidential patient data and to provide timely notice of a breach of such data would result in injury to Plaintiffs and the members of the proposed classes. Specifically, it was foreseeable that the failure to adequately safeguard confidential patient data would result in one or more of the following injuries to Plaintiffs and the members of the proposed classes: 1) the ongoing, imminent, certainly impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm; 2) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm; 3) the loss of the confidentiality of the compromised patient data; 4) the illegal sale of the compromised patient data on the Internet black market; 5) expenses for credit monitoring and identity theft insurance; 6) monetary damages in the form of

overpayment for services rendered; and 7) lost work time, and other economic and non-economic harm.

158. Defendants assumed the duty to use reasonable security measures as a result of their general conduct, internal policies and procedures, and their written Code of Conduct and Statement of Beliefs, in which the Defendants state that they are "dedicated to compliance with all federal, state and local laws, rules, and regulations, **including privacy and security of patient health information.**" Defendants have indicated in their published Code of Conduct that "**We consider patient information highly confidential**." Through these statements, Defendants specifically assumed the duty to comply with industry standards in protecting confidential patient data.

159. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and the Plaintiffs and the members of the proposed classes. The special relationship arose because Plaintiffs and the members of the proposed classes entrusted Defendants with their confidential patient data, as part of the health treatment process. Only Defendants were in a position to ensure that their systems were sufficient to protect against the harm to Plaintiffs and the members of the proposed classes from a data breach.

160. Defendants' duty to use reasonable security measures arose under HIPAA, pursuant to which Defendants are required to "reasonably protect" confidential patient data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential patient data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

161. Defendants' duty to use reasonable security measures arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential patient data by healthcare providers like Defendants. The FTC publications and data security breach orders described above further form the basis of Defendants' duty. In addition, individual states have enacted statutes based upon the FTC Act that also create a duty.

162. Defendants' duty to use reasonable care in protecting confidential patient data arose not only as a result of the common law and the statutes and regulations described above, but also because they were bound by, and had committed to comply with, industry standards for the protection of confidential patient data.

163. Defendants breached their common law, statutory and other duties - and thus were negligent - by failing to use reasonable measures to protect their patients' confidential data from the hackers and by failing to provide timely notice of the breach. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and proposed class members' confidential patient data;

b. failing to adequately monitor the security of their networks;

c. allowing unauthorized access to Plaintiffs' and the proposed class members' confidential patient data;

d. failing to recognize in a timely manner that Plaintiffs' and proposed class members' confidential patient data had been compromised;

e. failing to warn Plaintiffs and the members of the National Class and the Alternate State Specific Classes in a timely manner that their confidential patient data had been compromised;

164. In connection with the conduct described above, Defendants acted wantonly, recklessly, and with complete disregard for the consequences.

165. As a direct and proximate result of Defendants' negligence, the Plaintiffs, the National Class and the Alternate State Specific Classes have suffered and continue to suffer injury, including: 1) the ongoing, imminent, certainly impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm; 2) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm; 3) the loss of the confidentiality of the compromised patient data; 4) the illegal sale of the compromised patient data on the Internet black market; 5) expenses for credit monitoring and identity theft insurance; 6) monetary damages in the form of overpayment for services rendered; and 7) lost work time, and other economic and non-economic harm.

166. For reasons set forth in detail elsewhere herein, Tennessee common law applies to the negligence claim of the National Class. However, if the National Class is not certified, the negligence claims of the Alternate State Specific Classes would be governed by the law of each state in which such state specific claims are brought.

COUNT V
NEGLINGENCE *PER SE*
(On behalf of the National Class and the Alternate State Specific Classes)

167. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein

168. HIPAA was designed to protect the privacy of personal medical information by limiting its disclosure. Specifically, under HIPAA, Defendants are required to "reasonably protect" confidential patient data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Additionally, under HIPAA, Defendants are obligated to provide notification of a breach of protected health information. 45 C.F.R. §§ 164.404 and 164.410. The confidential patient data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

169. HIPAA seeks to protect the privacy of protected confidential patient data by prohibiting any voluntary or involuntary use or disclosure of such data in violation of the directives set out in the statute and its regulations, and requiring notification in all instances when such data is breached.

170. Defendants are HIPAA-covered entities.

171. As described above, Defendants violated HIPAA by failing to maintain the confidentiality of their protected health information and to provide timely notification of the breach of such data.

172. Defendants' violation of HIPAA constitutes negligence *per se*.

173. The Plaintiffs, the members of the National Class and the Alternate State Specific Classes, are part of the class of persons HIPAA was intended to protect as they are current or former patients of Defendants' healthcare network who provided protected health information to Defendants.

174. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the

FTC, the unfair act or practice of business of failing to use reasonable measures to protect confidential patient data.

175. Defendants violated Section 5 of the FTC Act (and similar state statutes, commonly the "Little FTC Acts," also known as state Unfair and Deceptive Trade Practices Acts)) by failing to use reasonable measures to protect confidential patient data and not complying with applicable industry standards, including HIPAA, as described in detail previously in this complaint. Defendants' conduct was particularly unreasonable given the nature and amount of confidential patient data it obtained and stored and the foreseeable consequences of a data breach of such data.

176. Defendants' duty to use reasonable security measures arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. Sec. 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential patient data by healthcare providers like Defendants. The FTC publications and data security breach orders described above further form the basis of Defendants' duty. In addition, the individual states have enacted statutes based upon the FTC Act that also create a duty.

177. Defendants violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se.*

178. The Plaintiffs, the National Class and the Alternative State Specific Classes are part of the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect as they are consumers who purchased healthcare services from Defendants.

179. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by the Plaintiffs and the members of the proposed classes.

180. As a direct and proximate result of Defendants' negligence *per se*, the Plaintiffs, and the members of the National Class and the Alternative State Specific Classes have suffered and continue to suffer injury, including:) the ongoing, imminent, certainly impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm; 2) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm; 3) the loss of the confidentiality of the compromised patient data; 4) the illegal sale of the compromised patient data on the Internet black market; 5) expenses for credit monitoring and identity theft insurance; 6) monetary damages in the form of overpayment for services rendered; and 7) lost work time, and other economic and non-economic harm.

181. For reasons set forth in detail elsewhere herein, Tennessee common law applies to the negligence *per se* claim of the National Class. However, if the National Class is not certified, the negligence *per se* claims of the members of the Alternate State Specific Classes would be governed by the law of each state in which such state specific claims are brought.

COUNT VI
BAILMENT
(On behalf of the National Class and the Alternate State Specific Classes)

182. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein.

183. Plaintiffs and the members of the National Class and the Alternate State Specific Classes delivered their confidential patient data to Defendants in order to receive healthcare services from Defendants' healthcare network.

184. This confidential patient data was furnished to Defendants for the exclusive purpose of administering and managing healthcare services delivered by Defendants' healthcare network, and Defendants took possession of the confidential patient data for the same reason.

185. Upon delivery, Plaintiffs and the members of the proposed classes intended and understood that Defendants would adequately safeguard their confidential patient data, and Defendants, in accepting possession, understood the expectations of Plaintiffs and the members of the proposed classes. Accordingly, bailment was established for the mutual benefit of the parties at the time of delivery and acceptance of possession.

186. Pursuant to the bailment arrangement, Defendants owed Plaintiffs and the members of the proposed classes a duty of reasonable care in safeguarding and protecting their confidential patient data.

187. This duty was breached by Defendants' failure to take adequate steps to protect the confidential patient data entrusted to them and Defendants' failure to conform to best practices and industry standards to prevent unauthorized access to Plaintiffs' and the proposed class members' confidential patient data.

188. As a direct and proximate result of Defendants' failure to fulfill their obligations under the bailment arrangement, the Plaintiffs and the members of the National Class and the Alternative State Specific Classes have suffered and continue to suffer injury, including: 1) the ongoing, imminent, certainly impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm; 2) actual identity theft crimes, fraud and abuse, resulting in

monetary loss and economic harm; 3) the loss of the confidentiality of the compromised patient data; 4) the illegal sale of the compromised patient data on the Internet black market; 5) expenses for credit monitoring and identity theft insurance; 6) monetary damages in the form of overpayment for services rendered; and 7) lost work time, and other economic and non-economic harm.

189. For reasons set forth in detail elsewhere herein, Tennessee common law applies to the bailment claim of the National Class. However, if the National Class is not certified, the bailment claims of the alternative state specific classes would be governed by the law of each state in which such state specific claims are brought.

COUNT VII
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT
(On behalf of the National Class)

190. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein.

191. The Fair Credit Reporting Act ("FCRA") "require[s] consumer reporting agencies [to] adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information." 15 U.S.C. § 1681(b).

192. The FCRA protects the disclosure of medical information and only allows dissemination in a limited number of circumstances. *See* 15 U.S.C. § 1681a(d)(3); § 1681b(g); § 1681(a)(6).

193. Plaintiffs' and the proposed class members' confidential patient data constitutes "medical information" for purposes of the FCRA.

194. Defendants are "consumer reporting agencies" because "for monetary fees, dues, [and/]or on a cooperative nonprofit basis, [they] regularly engage[] in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and [] use . . . interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f). Defendants are in the business of assembling personal and medical information about Plaintiffs and other consumers and providing reports with this information to third parties.

195. Defendants' collection of Plaintiffs' and the proposed class members' confidential patient data and subsequent transmission and communication of the same constitutes a "consumer report" because the information collected "bear[s] on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" and "is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes." 15 U.S.C. § 1681a(d)(1). Defendants collect personal, medical and financial information and prepare reports of the same to extend credit for healthcare services, collect debt or determine eligibility for insurance.

196. Defendants, as consumer reporting agencies, were required (and still are required) to put in place and maintain procedures that would protect the confidential patient data of Plaintiffs and the proposed members of the classes and limit its disclosure exclusively to those situations outlined in the FCRA. Defendants failed to put in place and/or maintain the requisite procedures and thereby caused Plaintiffs' and the proposed class members' information to be

disclosed in violation of the FCRA, directly resulting in the theft and wrongful dissemination of that information.

197. Defendants' violation was willful and/or reckless because Defendants were aware of their obligations to protect the confidential patient data at issue and knew or acted in reckless disregard of whether their conduct would result in the wrongful dissemination of that information, resulting in a violation of the FCRA.

198. As a direct and proximate result of Defendants' willful violation of the FCRA, the Plaintiffs and the members of the National Class have suffered and continue to suffer injury, including: 1) the ongoing, imminent, certainly impending threat of identity theft crimes, fraud and abuse; 2) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm; 3) the loss of the confidentiality of the compromised patient data; 4) the illegal sale of the compromised patient data on the Internet black market; 5) expenses for credit monitoring and identity theft insurance; 6) monetary damages in the form of overpayment for services rendered; and 7) lost work time, and other economic and non-economic harm.

199. Thus, Plaintiffs and the members of the National Class are entitled to statutory damages, non-statutory damages in an amount to be proven at trial, and attorneys' fees.

COUNT VIII
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT
(On behalf of the National Class)

200. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein.

201. In the alternative to their claim for willful violation of the FCRA, Plaintiffs and the members of the National Class allege that Defendants negligently violated the FCRA by failing to adequately protect the confidential patient data of Plaintiffs and the members of the

National Class, to put in place and maintain procedures designed to protect Plaintiffs' and the proposed class members' confidential patient data, and to limit their disclosure of such information solely to the situations outlined in the FCRA.

202. As described above, this failure proximately caused the theft and wrongful dissemination of the confidential patient data, in violation of the FCRA.

203. It was reasonably foreseeable that Defendants failure to put in place and maintain procedures to protect and limit the disclosure of Plaintiffs' and the proposed class members' confidential patient data would result in the theft, unlawful dissemination and/or wrongful disclosure of the data, in violation of the FCRA.

204. Defendants' violation of the FCRA was negligent.

205. As a direct and proximate result of Defendants' negligent violation of the FCRA, the Plaintiffs and the members of the National Class have suffered and continue to suffer injury, including: 1) the ongoing, imminent, certainly impending threat of identity theft crimes, fraud and abuse; 2) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm; 3) the loss of the confidentiality of the compromised patient data; 4) the illegal sale of the compromised patient data on the Internet black market; 5) expenses for credit monitoring and identity theft insurance; 6) monetary damages in the form of overpayment for services rendered; and 7) lost work time, and other economic and non-economic harm.

206. Thus, Plaintiffs and the members of the National Class are entitled to statutory damages, non-statutory damages in an amount to be proven at trial and attorneys' fees.

COUNT IX
VIOLATION OF STATE CONSUMER LAWS
(On behalf of the State Statutory Classes)

207. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set out herein.

208. Plaintiffs and members of the State Statutory Classes are current or former patients of Defendants who provided confidential patient data to Defendants as part of the purchase of personal healthcare services from Defendants.

209. Defendants engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of goods or services to consumers, including Plaintiffs and members of the classes.

210. Defendants are engaged in, and its acts and omissions affect, trade and commerce. Defendants' acts, practices, and omissions were done in the course of Defendants' business of marketing, offering for sale, and selling goods and services throughout the United States.

211. Defendants' conduct constitutes unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices (collectively, "Unfair or Deceptive Trade Practices"), including, among other things, Defendants':

a. failure to maintain adequate computer systems and data security practices to safeguard customers' confidential patient data;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard customers' confidential patient data from theft;

c. failure to timely and accurately disclose the data breach to Plaintiffs and the members of the State Statutory Classes;

d. continued acceptance of Plaintiffs' and the State Statutory Class members' confidential patient data after Defendants knew or should have known of the security vulnerabilities that were exploited in the data breach; and

e. continued acceptance of Plaintiffs' and the State Statutory Class members' confidential patient data after Defendants knew or should have known of the data breach.

212. By engaging in such Unfair or Deceptive Trade Practices, Defendants have violated state consumer laws, including those that prohibit:

a. representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;

b. representing that goods and services are of a particular standard, quality or grade, if they are of another;

c. omitting material facts regarding the goods and services sold;

d. engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding;

e. unfair methods of competition;

f. unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices; and/or

g. similar prohibitions under the state consumer laws identified below.

213. As a direct and proximate result of Defendants violating state consumer laws, Plaintiffs and the State Statutory Class members suffered one or more of the following damages:

a. the ongoing, imminent, certainly impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm;

b. actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm;

c. the loss of the confidentiality of the compromised patient data;

d. the illegal sale of the compromised patient data on the Internet black market;

e. expenses for credit monitoring and identity theft insurance;

f. monetary damages in the form of overpayment for services rendered, based on purchasing services from Defendants that they would not have purchased, or would have not had paid the same price for, had they known of Defendants' Unfair or Deceptive Trade Practices; and

g. lost work time, and other economic and non-economic harm.

214. Defendants' Unfair or Deceptive Trade Practices violate the following state consumer statutes:

a. The Arizona Consumer Fraud Act, A.R.S. § 44-1522;

b. The Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-107(a)(1)(10) and 4-88-108(1)(2), *et seq.*;

c. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), *et seq.*;

d. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Stat. § 505/2, *et seq.*, and the Illinois Uniform Deceptive Trades Practices Act, 815 Ill. Stat. §§ 510/2(a)(5), (7) and (12), *et seq.*;

e. The Indiana Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5-3(a) and (b)(1) and (2), *et seq.*;

f. The Kentucky Consumer Protection Act, Ky. Rev. Stat. §§ 367.170(1) and (2), *et seq.*;

g. The Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), *et seq*;

h. The Revised Statutes of Nebraska, Neb. Rev. Stat. § 87.302, *et seq.*;

i. The New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, *et seq.*;

j. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2(D)(5)(7) and (14) and 57-12-3, *et seq.*;

k. The Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. §§ 1345.02(A) and (B)(1) and (2), *et seq.*;

l. The Oklahoma Consumer Protection Act, 15 Okl. Stat. Ann. §§ 753(5), (7) and (20), *et seq.*;

m. The Oregon Unfair Trade Practices Act, Or. Rev. Stat. §§ 646.608(1)(e)(g) and (u), *et seq.*;

n. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-2(4)(v)(vii) and (xxi), and 201-3, *et seq.*;

o. The Texas Deceptive Trade Practices Consumer Protection Act, V.T.C.A., Bus. & C. §§ 17.46(a), (b)(5) and (7), *et seq.*;

p. The Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020, *et seq.*; and

q. The West Virginia Consumer Credit and Protection Act, W.V.A. Code § 46A-6-104, *et seq*.

215. As a result of Defendants' violations, Plaintiffs and members of the State Statutory Classes are entitled to injunctive relief, including, but not limited to: (1) ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors; (2) ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring; (3) ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Defendants segment patient data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems; (5) ordering that Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services; (6) ordering that Defendants conduct regular database scanning and securing checks; (7) ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (8) ordering Defendants to meaningfully educate their patients about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Defendants' patients must take to protect themselves.

216. Because of Defendants' unfair or deceptive trade practices, Plaintiffs and the members of State Statutory Classes are entitled to relief, including restitution of the costs associated with the data breach, disgorgement of all profits accruing to Defendants because of its Unfair or Deceptive Trade Practices, attorneys' fees and costs, declaratory relief, and a permanent injunction enjoining Defendants from its Unfair or Deceptive Trade Practices.

217. Plaintiffs bring this claim on behalf of themselves and the members of the State Statutory Classes for the relief requested and to benefit the public interest. This claim supports the public interests in assuring that consumers are provided truthful, non-deceptive information about potential purchases of services and protecting members of the public from Defendants' Unfair or Deceptive Trade Practices. Defendants' unfair and wrongful conduct, including its Unfair or Deceptive Trade Practices has affected the public at large.

218. Before filing this Complaint, counsel for Plaintiffs and the members of the State Statutory Classes provided Defendants with pre-suit demand letters in compliance with state consumer laws Tex. Bus. & Com. Code Ann. § 17.505(a) and W.Va. Code § 46A-6- 106(b). Additionally, Defendants have had long notice of Plaintiffs' allegations, claims, and demands based on the numerous class actions related to this litigation.

219. Plaintiffs have provided or will provide notice of this action and a copy of this Complaint to the appropriate Attorneys General.

COUNT X
VIOLATION OF STATE DATA BREACH NOTIFICATION STATUTES
(On behalf of the State Statutory Classes)

220. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein.

221. Legislatures in the states and jurisdictions listed below have enacted data breach statutes. These statutes generally apply to any person or business conducting business within the state that owns or licenses computerized data containing personal information. If the personal information is acquired or accessed in a way that compromises its security or confidentiality, the covered entity must notify the affected individuals in the most expedient time and manner possible and without unreasonable delay.

222. The Defendants' data breach constituted a security breach that triggered the notice provisions of the data breach statutes and the confidential patient data taken includes categories of personal information protected by the data breach statutes.

223. Defendants unreasonably delayed in informing Plaintiffs and members of the State Statutory Classes about the data breach after Defendants knew or should have known that the data breach had occurred.

224. Plaintiffs and State Statutory class members were damaged by Defendants' failure to comply with the data breach statutes.

225. Had Defendants provided timely and accurate notice, Plaintiffs and the members of the State Statutory classes could have avoided or mitigated the harm caused by the data breach. For example, they could have contacted their banks to change account numbers, taken security precautions in time to prevent or minimize identity theft, or contacted governmental authorities.

226. Defendants' failure to provide timely and accurate notice of the Defendants' data breach violated the following state data breach statutes:

a. Ga. Code Ann. § 10-1-912(a), *et seq.*;

b. Ill. Comp. Stat. Ann. 530/10(a), *et seq.*;

c. Ky. Rev. Stat. Ann. § 365.732(2), *et seq.*;

d. La. Rev. Stat. Ann. § 51:3074(A), *et seq.*;

e. N.J. Stat. Ann. § 56:8-163(a), *et seq.*;

f. Or. Rev. Stat. Ann. § 646A.604(1), *et seq.*;

g. S.C. Code Ann. § 39-1-90(A), *et seq.*;

h. Tenn. Code Ann. § 47-18-2107(b), *et seq.*;

i. Va. Code Ann. § 18.2-186.6(B), *et seq.*; and

j. Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*

227. Plaintiffs and members of each of the State Statutory Classes seek all remedies available under their respective state data breach statutes, including but not limited to damages, equitable relief, including injunctive relief, treble damages, and reasonable attorneys' fees and costs, as provided by the applicable laws.

COUNT XI
WANTONNESS
(On behalf of the National Class and the Alternate State Specific Classes)

228. Plaintiffs incorporate and re-allege each and every allegation as if fully set forth herein.

229. Defendants knew, were substantially aware, should have known, or acted in reckless disregard that Plaintiffs would be harmed if Defendants did not safeguard, secure, protect, keep private, and not disclose Plaintiffs' confidential patient data.

230. Defendants did not safeguard, secure, keep private, and/or protect and disclosed to third-parties Plaintiffs' and class members confidential patient data with a knowledge or consciousness that the action or failure to act will likely or probably cause harm or, in the alternative, with reckless indifference to the consequences.

231. As a direct and proximate result of Defendants' conduct, the Plaintiffs and the members of the National Class and the Alternative State Specific Classes have suffered and continue to suffer injury, including: 1) the ongoing, imminent, certainly impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm; 2) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm; 3) the loss of the confidentiality of the compromised patient data; 4) the illegal sale of the compromised patient data on the Internet black market; 5) expenses for credit monitoring and identity theft insurance; 6) monetary damages in the form of overpayment for services rendered; and 7) lost work time, and other economic and non-economic harm.

232. For reasons set forth in detail elsewhere herein, Tennessee common law applies to the wantonness claim of the National Class. However, if the National Class is not certified, the wantonness claims of the alternative state specific classes would be governed by the law of each state in which such state specific claims are brought.

PRAYER FOR RELIEF

233. Plaintiffs request that this Court enter judgment against Defendants and in favor of Plaintiffs and the members of the proposed classes and award the following relief:

a) That this action be certified as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, declaring Plaintiffs as the representatives of the classes/subclasses defined herein and Plaintiffs' counsel as counsel for such classes/subclasses;

b) Monetary damages;

c) Injunctive relief, including but not limited to the provision of credit monitoring services for Plaintiffs and the members of the proposed

classes for a period of at least twenty-five (25) years, the provision of bank monitoring services for Plaintiffs and the members of the proposed classes for a period of at least twenty-five (25) years, the provision of credit restoration services for Plaintiffs and the members of the proposed classes for a period of at least twenty-five (25) years, and the provision of identity theft insurance for Plaintiffs and the members of the proposed classes for a period of at least twenty-five (25) years;

d) Reasonable attorneys' fees and expenses, including those related to experts and consultants;

e) Costs;

f) Pre- and post-judgment interest;

g) Such other relief as this Court may deem just and proper.

JURY DEMAND

234. Pursuant to Fed. R. Civ. P. 38(b), Plaintiffs, individually and on behalf of the classes they seek to represent, demand a trial by jury for all issues so triable.

Dated: July 20, 2015

By: s/ Karen Hanson Riebel

Friedman, Dazzio, Zulanas & Bowling, P.C.
Jeffrey E. Friedman
Christopher J. Zulanas
John Michael Bowling
3800 Corporate Woods Drive
Birmingham, AL 35242
jfriedman@friedman-lawyers.com
czulanas@friedman-lawyers.com
mbowling@friedman-lawyers.com

Lockridge Grindal Nauen P.L.L.P.
Karen Hanson Riebel
Kate M. Baxter-Kauf
100 Washington Ave. S.

Suite 2200
Minneapolis, MN 55113
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

Plaintiffs' Co-Lead Counsel

Pittman, Dutton, Hellums, P.C.
Christopher T. Hellums
2001 Park Pl, #1100
Birmingham, AL 35203
chrish@pittmandutton.com

Plaintiffs' Liaison Counsel

Carlson Lynch Sweet & Kilpela
Gary F. Lynch
Edwin J. Kilpela
Jamisen A. Etzel
PNC Park
115 Federal Street, Suite 210
Pittsburg, PA 15212
glynch@carlsonlynch.com
ekilpela@carlsonlynch.com
jetzel@carlsonlynch.com

Wood Law Firm LLC
Kirk Wood
PO Box 382434
Birmingham, AL 35238
kirk@woodlawfirmllc.com

Beasley Allen Crow Methvin Portis & Miles PC
Andrew E. Brashier
Gibson Vance
Julia A. Beasley
W. Daniel Miles
218 Commerce Street
Montgomery, AL 36104
Andrew.Brashier@beasleyallen.com
gibson.vance@beasleyallen.com
julia.beasley@beasleyallen.com
dee.miles@beasleyallen.com

Goldman Scarlato & Penny, P.C.
Brian Penny
Mark Goldman
101 E. Lancaster Ave., Suite 204
Wayne, PA 19087
penny@lawgsp.com
goldman@lawgsp.com

Lite DePalma Greenberg, LLC
Katrina Carroll
212 W. Wacker Drive, Suite 500
Chicago, IL 60606
kcarroll@litedepalma.com

Slack & Davis LLP
Paula Knippa
2705 Bee Cave Road, Suite 220
Austin, TX 78746
pknippa@slackdavis.com

McCallum Methvin & Terrell PC
Robert Methvin
James M. Terrell
2201 Arlington Avenue South
Birmingham, AL 35205
rgm@mmlaw.net
jterrell@mmlaw.net

Plaintiffs' Steering Committee

Stewart & Stewart PC
Donald W. Stewart
Greg Foster
Dylan Reeves
1826 3rd Avenue North, Suite 300
Bessemer, AL 35021
donaldwstewart5354@yahoo.com
greg@stewartandstewart.net
dreeves@stewartandstewart.net

Caroselli, Bleacher, McTiernan & Conboy LLC
William R. Caroselli
David S. Senoff
20 Stanwix Street, 7th Floor
Pittsburgh, PA 15222
wcaroselli@cbmclaw.com
dsenoff@cbmclaw.com

Clanton Legal Group PLLC
Bradley S. Clanton
P.O. Box 4781
Jackson, MS 39296
brad@clantonlegalgroup.com

Tatum & Wade PLLC
Joe N. Tatum
124 East Amite Street
Jackson, MS 39201
jntatum@aol.com

The Giatras Law Firm, PLLC
Troy N. Giatras
Matthew W. Stonestreet
118 Capitol Street, Suite 400
Charleston, WV 25301
troy@thewvlawfirm.com
matt@thewvlawfirm.com

James F. Humphreys & Associates, L.C.
James F. Humphreys
10 Hale Street Suite 400
Charleston, WV 25301
jhumphreys@jfhumphreys.com

Branch Law Firm
Turner W. Branch
Mary Lou Boelcke
2025 Rio Grande Blvd NW
Albuquerque, NM 87104
tbranch@branchlawfirm.com
mlboelcke@branchlawfirm.com

Dogali Law Group, PA
Andy Dogali
Geoff E. Parmer
101 E. Kennedy Blvd, Suite 1100
Tampa, FL 33602
adogali@dogalilaw.com
gparmer@dogalilaw.com

Gilbert Russell McWherter Scott & Bobbit PLC
Clinton H. Scott
101 North Highland Ave
Jackson, TN 38301
cscott@gilbertfirm.com

The Buxner Law Firm
Evan Buxner
230 S. Bemiston Avenue, Suite 500
St. Louis, MO 63105
ebuxner@buxnerlaw.com

Estes Gramling & Estes PLC
Doug Gramling
19 E. Dickson Street
Fayetteville, AR 72701
dgramling@egelaw.com

WM Eric Colley
Eric Colley
PO Box 681045
Fort Payne, AL 35967
colleyw@bellsouth.net

Garson Johnson LLC
Jeffrey D. Johnson
Jim A. DeRoche
101 W. Prospect Ave
Midland Building, Suite 1610
Cleveland, OH 44115
jjohnson@garson.com
jderoche@garson.com

Karon LLC
Daniel Karon
Beau D. Hollowell
700 W. Saint Clair Ave., Suite 200
Cleveland, OH 44113
dkaron@karonllc.com
bhollowell@karonllc.com

The Scott Law Group PS
Matthew Zuchetto
Darrell W. Scott
926 West Sprague, Suite 680
Spokane, WA 99201-5076
matthewzuchetto@me.com
darrellscott@me.com

Robert Peirce & Associates PC
Aaron Rihn
2500 Gulf Tower
707 Grant Street
Pittsburgh, PA 15219
arihn@peircelaw.com

Medure Bonner Bellissimo Peirce & Daley LLC
Jason A. Medure
Joseph Bellissimo
Michael Bonner
22 North Mill Street
New Castle, PA 16101
jmedure@medurebonnerlaw.com
jsblaw@prodigy.net
mbonner@medurebonnerlaw.com

M. Adam Jones & Associates LLC
Mark Adam Jones
Jordan S. Davis
206 N. Lena Street
Dothan, AL 36303
adam@adamjoneslaw.com
Jordan@adamjoneslaw.com